The Technology Split in Customer List Interpretation

Alan E. Littmann†

A "technology split" has developed among courts over the treatment of customer lists. Although courts for years have held that companies' customer data is freely alienable,[1] recent cases involving Internet companies imply otherwise.[2] Customer advocates, academics, regulators, and legislators are now pointing to the Internet as the final battleground for privacy.[3] Members of these groups warn that personal information may be gleaned from customers' online activities and used to steal their identities,[4] expose their children to sexual predators,[5] or reveal their private medical conditions.[6]

---

† A.B. 1996; J.D. Candidate 2003, The University of Chicago.

1 See John D. Penn, *Internet Privacy: An Oxymoron*, 2000 ABI J Lexis 81, *6 (describing the privacy debate about customer lists and noting that "[l]ost in the debate is the fact that customer lists and other information provided by customers have been bought and sold for decades"). See also Robert L. Eisenbach III, *The Internet Company's Customer List: Asset or Liability?*, 18 Computer & Internet Law 25, 25 (2001) ("In the 'bricks and mortars' world, customer lists are bought and sold regularly.").

2 For instance, the bankruptcy of Toysmart.com and the cases that came in its wake imply a significant restriction on selling customer lists. See Richard A. Beckmann, Comment, *Privacy Policies and Empty Promises: Closing the "Toysmart Loophole,"* 62 U Pitt L Rev 765, 765–70 (2001) (providing a summary of the Toysmart.com litigation and the concerns of both sides of the debate and noting that "[b]ankruptcy is the most recent battleground in the struggle between customers and businesses over control of personal information").

3 See Editorial, *Protecting Online Privacy*, NY Times A18 (May 20, 2002) (advocating the passage of the Online Personal Privacy Act because it would "give individuals more control" over their private information).

4 For a general discussion, see Prepared Statement of the Federal Trade Commission before the Senate Committee on Commerce, Science, and Transportation, *Online Profiling—Benefits and Concerns*, 1236 PLI/Corp 297 (2001) (warning that companies can use customer information to create profiles of people and apply for credit cards and otherwise transact under their identities). See also Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 Mich Telecomm & Tech L Rev 97, 111–12 (2001) (noting that "identity thieves have gone on shopping sprees at the expense of their victims" and that "the possibilities for abuse through identity theft will grow as the functionality of the Internet expands"); Brandon McKelvey, Comment, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft*, 34 UC Davis L Rev 1077, 1082 (2001) ("A financial institutions' collection and use of personal information directly connects them with the growing problem of identity theft.").

5 See Hetcher, 7 Mich Telecomm & Tech L Rev 97 at 112 (cited in note 4) ("Another type of harm that has received a good deal of attention is predation on children."); Federal Trade Commission, *Privacy Online: A Report to Congress* 5 (June 1998), available online at <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (visited June 12, 2002) (citing a Justice Department investigation revealing that online services and bulletin boards are "quickly becoming the most powerful resources used by predators to identify and contact children," as well as anec-

While these concerns may be real, they are certainly not new. Offline companies' customer lists have been collected and sold regularly.[7] Courts, therefore, need to filter through the rhetoric when dealing with the seemingly new phenomenon of Internet customer lists. Courts should maintain the sound legal analysis that has been applied to companies' ownership of customer lists for years—and that continues to be applied outside of cyberspace.

This Comment argues that recent court decisions and high-profile settlements have unnecessarily distinguished between "online" and "offline" companies,[8] creating a "technology split." This distinction is harmful because it is both unenforceable and counterproductive. Rather than distinguishing on the basis of technology, courts should treat customer lists uniformly across companies and follow the extensive pre-Internet case law on customer lists.

Part I describes customer lists and the current controversy over their use by Internet companies. Part II reviews the treatment of customer lists in the case law. Part III compares Internet customer lists with traditional lists and argues that separate, nonuniform treatment is unwarranted. Part IV explains why this separate treatment is actually harmful to both companies and customers. Finally, Part V proposes guidelines for handling future customer list cases.

I. CUSTOMER LISTS AND PRIVACY

This Part presents an overview of customer lists and the manner in which they have historically been gathered and used. New technology gives companies increased capabilities for collecting customer lists and this Part discusses how these new capabilities have created concern over privacy rights.

A. What Are Customer Lists?

A customer list is much more than the name suggests.[9] In addition to compiling the names of previous or prospective customers,[10] a com-

---

dotal evidence that children in web chatrooms increasingly receive inappropriate advances from adults).

6 See Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* 10–12 (O'Reilly 2000).

7 See Eisenbach, *Internet Company's Customer List* at 25 (cited in note 1).

8 While these are inappropriate labels, for reasons stated in Part III.D, this Comment will continue to use them for the sake of simplicity.

9 Customer lists should not be confused with other privacy issues such as the fight against Carnivore, which is not within the scope of this Comment. Carnivore is an Internet monitoring system developed by the FBI that allegedly is able to filter Internet traffic and deliver suspicious information to the FBI. See Thomas R. McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 Mo L Rev 827, 828–89 (2001).

10 See, for example, *In re McGee*, 157 Bankr 966, 971, 975 (E D Va 1993) (involving a cus-

pany may gather a significant amount of personal information that helps explain its customers' preferences and spending habits. For example, American Express for years has collected extensive information about the spending habits of its customers.[11] Before its demise in 2000, online toy retailer Toysmart.com collected similar information, such as customers' "billing information, shopping preferences, and family profiles."[12] CVS, Kmart, and Wal-Mart also participated in a plan whereby they combined their sales data from stores worldwide and sold the data to marketing companies and drugmakers.[13]

A company can create tremendous value by using a customer list for cross-marketing efforts. For instance, information that a company gathers from selling cookbooks can be used to identify customers who are also interested in purchasing the company's kitchen supplies. Third parties are also potential purchasers of customer information.[14] A backpacking equipment retailer, for example, might find the subscription list to *Backpacker* magazine tremendously valuable. The more detailed and extensive the list is, the more valuable it becomes.[15]

B. New Technology, New Capabilities, New Dangers?

The Internet has brought a new wave of controversy over the collection and sale of customer lists.[16] Customer groups and commenta-

---

tomer list that contained a "list of vendors across the country," and discussing another case involving a list of customers).

11 See *Dwyer v American Express Co*, 273 Ill App 3d 742, 652 NE2d 1351, 1353 (1995) (describing how defendants "categorize and rank their card holders into ... tiers based on spending habits" for the purpose of which they "analyze where [customers] shop and how much they spend, ... behavior characteristics and spending histories"). See also Jeff Sweat, *Privacy: Can Businesses Build Trust and Exploit Opportunity?*, InformationWeek.com (Aug 20, 2001), available online at <http://www.informationweek.com/story/IWK20010817S0004> (visited May 30, 2002) (describing how Harrah's "records how often a person stays at a hotel, even the kind of room he or she prefers").

12 Federal Trade Commission, Press Release, *FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors* (July 10, 2000), available online at <http://www.ftc.gov/opa/2000/07/toysmart.htm> (visited Feb 5, 2002).

13 See John Rendleman, *Customer Data Means Money*, InformationWeek.com (Aug 20, 2001), available online at <http://www.informationweek.com/story/IWK20010816S0008> (visited June 12, 2002).

14 A rough estimate is that companies will pay about $150 per 1,000 names. See id.

15 See, for example, *Dwyer*, 652 NE2d at 1353 (describing how American Express would "offer to create a list of cardholders who would most likely shop in a particular store" or "who purchase specific types of items" and "rent that list to the merchant"). Companies can also increase the value of their customer list by categorizing customers, which enables buyers of the list to target those customers more effectively in a particular marketing demographic. A company can place the customer information in a database and sort and categorize it according to numerous factors that might be of interest to a buyer. By investing in the list itself, the company can create an asset that is significantly more valuable than a mere list of customer information.

16 See Sean Doherty, *Keeping Data Private*, Network Computing 83, 83 (June 25, 2001) ("Potential customers hesitate to part with private information on the Internet when they don't know how the information will be used and who will be using it. Jupiter Research estimates that

tors point out that the Internet has reduced the cost of both gathering customer information and using it to target new customers.[17] Companies using the Internet can gather more specific, and potentially more intrusive, information than their offline counterparts.[18] For instance, while traditional companies could only discover what a customer purchased, online companies can record what products consumers browsed—even if they eventually chose not to buy.[19] By using cookie technology, website owners can monitor what products a user browsed, thereby allowing analysts to deduce customers' interests even if they do not purchase anything.

The increased volume of information collected by Internet companies has led to a rash of warnings that customer privacy and safety may be in jeopardy. Some customer advocates fear that gathering customer information will lead to predation on children, identity theft, or the illicit use of medical information.[20] Customer advocates also fear that companies will share this information with political groups or other potentially sensitive and intrusive organizations.[21]

The Federal Trade Commission ("FTC"), concerned by the additional capabilities that online companies possess through their use of technology, now regularly monitors online privacy.[22] Numerous articles

---

Internet-related business will lose $18 billion in unrealized transactions because of privacy concerns by 2003."); TRUSTe, *TRUSTe Guidelines on Personally Identifiable Information Uses in Mergers, Acquisitions, Bankruptcies, Closures, and Dissolutions of Web Sites* (submitted for public comment Apr 11, 2001), available online at <http://www.truste.com/programs/mabs.doc> (visited Oct 3, 2002) (describing the Internet era as one "marked by increasing customer vigilance over privacy" and urging that "in an increasingly connected world, customers must have mechanisms that give them full control over their personal, private information so that they can protect their privacy"). See also Kate Miller, *TRUSTe Unveils Privacy Guidelines*, Industry Standard (Apr 12, 2001) (quoting privacy concerns voiced by TRUSTe and an analyst at the Electronic Privacy Information Center).

17 See Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, 16 No 5 Computer Law 7, 7 (May 1999) (arguing that the Internet has influenced privacy by reducing the cost of information and improving the ability of companies to target customers).

18 See id.

19 See id (describing "cookie" technology and noting that, "New technology and more powerful computers now make it possible, without the visitor's knowledge, for companies to record and track information about visitors to their websites, including . . . which portions of the site were visited and for how long.").

20 See Hetcher, 7 Mich Telecomm & Tech L Rev 97 at 6 (cited in note 4) (discussing potential misuses of customer information); Garfinkel, *Database Nation* at 10–12 (cited in note 6); Federal Trade Commission, *Privacy Online: A Report* at 5 (cited in note 5).

21 See Aaron Pressman, *Voter.com to Sell Membership List*, Industry Standard (Mar 15, 2001), available online at <http://www.thestandard.com/article/0,1902,22894,00.html> (visited June 12, 2002) (describing how an Internet portal for politics attempted to sell the political party affiliations of its members).

22 The FTC now issues annual reports about online privacy. See Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* 3–5 (May 2000) (discussing the three reports on online privacy that the FTC submitted to Congress in 1998–2000).

have also stressed the need for additional regulation of the Internet and have urged courts and legislators to force companies to respect the privacy rights of their customers.[23] Some commentators even advocate allocating property rights in personal information to customers.[24]

Internet companies, in turn, have responded to increased privacy concerns by placing disclosures on their websites notifying visitors how their personal information will be used.[25] These disclosures, however, have done little to alleviate customer concerns. In fact, a recent survey showed that few consumers trust online disclaimers; 92 percent of respondents agreed with the statement, "I don't trust companies to keep personal information about me confidential, no matter what they promise."[26]

C. A Reason for Skepticism

Customers may have good reason not to trust Internet companies' privacy policies. The policies are often ambiguous.[27] For example, LexisNexis provides the following catchall disclaimer:

> Circumstances may arise where we are required to disclose your personal information to third parties for purposes other than to support your customer relationship . . . , such as in connection with a corporate divestiture or dissolution . . . or if disclosure is required by law or is pertinent to judicial or governmental investigations or proceedings.[28]

---

23 See Editorial, *Protecting Online Privacy*, NY Times at A18 (cited in note 3).

24 See, for example, Jessica Litman, *Information Privacy/Information Property*, 52 Stan L Rev 1283, 1289–95 (discussing the various arguments for protecting data privacy with property rights).

25 For example, on its website, <http://www.lexisnexis.com/terms/privacy> (visited Apr 6, 2002), LexisNexis states in part:

> Our Web Site is not set up to automatically collect personally identifiable information from each visitor to our Web Site. It does recognize the home server of visitors, but not e-mail addresses. . . . This information is used only for internal purposes by our technical support staff. . . . Our Web Site does track certain information about the visits to our Web Site. . . . [LexisNexis] may enhance or merge your information collected at its Web Site with data from third parties for purposes of marketing products or services to you.

26 Steve Lohr, *Survey Shows Few Trust Promises on Online Privacy*, NY Times C4 (Apr 17, 2000) (discussing a 2000 survey of 3000 U.S. households conducted by the market research firm Odyssey).

27 See William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 NYU L Rev 1812, 1812 (2001) ("Privacy policies of typical sites . . . contain hidden, verbose, jargon-cluttered statements that provide little guidance about the practices of the site's operator.").

28 LexisNexis Privacy Statement <http://www.lexisnexis.com/terms/privacy> (visited Apr 6, 2002).

Even the companies that display these warnings often seem to ignore them blatantly. The most famous example of disregard is described in *In re Toysmart.com*.[29]

Web retailer Toysmart.com, founded in 1998, started out as a moderate success, achieving more than $6 million in sales in December 1999.[30] During this time, Toysmart.com had a privacy policy that assured customers of the company's commitment to privacy and specifically stated that customer information would "never be shared with a third party."[31]

Toysmart.com's tactics shifted, though, when it ran into financial trouble. After Toysmart.com entered bankruptcy in 2000, it began searching for a company to buy its customer list.[32] By seeking to sell the customer list, it sought only to maximize the value of its bankruptcy estate in order to pay its creditors. However, consumer advocates and politicians were outraged.[33] Toysmart.com was excoriated in the media for allegedly violating its customers' privacy and for disregarding previous promises.[34] The FTC responded by filing a complaint that sought to enjoin the sale.[35] The complaint charged Toysmart.com

---

29 Petition for involuntary bankruptcy, Chapter 11 Case No 00-13995-CJK (Bankr D Mass filed June 9, 2000).

30 Glenn R. Simpson, *FTC Is Set to Challenge Toysmart.com to Prevent the Sale of Customer Data*, Wall St J A3 (July 10, 2000).

31 See Federal Trade Commission, Press Release, *FTC Sues* (cited in note 12). The policy read in full:

> Personal information, voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. . . . When you register with Toysmart.com, you can rest assured that your information will never be shared with a third party.

32 Upon filing, Toysmart.com listed $10.5 million in assets, including the customer list, and liabilities of $29 million. See Motion for Authority to Sell Inventory by Private Sale Free and Clear of Liens, Claims and Encumbrances, *In re Toysmart.com*, Chapter 11 Case No 00–13995–CJK (D Mass filed June 23, 2000). While it was not clear how much the list was worth, estimates placed the number of individuals on the list at approximately 250,000. See Matt Richtel, *Toysmart.com in Settlement with F.T.C.*, NY Times C1 (July 22, 2000). See also Greg Sandoval, *Failed Dot-Coms May Be Selling Your Private Information*, News.com (June 29, 2000), available online at <http://news.com.com/2100–1017–242649.html?legacy=cnet> (visited Feb 15, 2002) (noting that Toysmart.com advertised the sale of its customer list and database in *The Wall Street Journal* after shutting down).

33 See generally Commentary, *Congress Needs to Pass Legislation to Protect Personal Data When Internet Companies Go Bankrupt*, San Jose Mercury News (Apr 9, 2001); Hal F. Morris and Flora A. Fearson, *Texas Attorney General: Privacy Is Not for Sale*, 2000 ABI J Lexis 86, *4 (arguing that companies have no right to sell customer lists in violation of their privacy statements).

34 See Commentary, *Congress Needs to Pass Legislation*, San Jose Mercury News (cited in note 33).

35 See First Amended Complaint for Permanent Injunction and Other Equitable Relief, *FTC v Toysmart.com*, Civil Action No 00-11341-RGS, available online at <http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm> (visited Feb 5, 2002).

with violating child protection laws[36] and engaging in deceptive practices in violation of Section 5(a) of the Federal Trade Commission Act.[37] Numerous state attorneys general also intervened, alleging the violation of state customer protection acts.[38]

In the face of the legal and political pressure, Toysmart.com and the FTC reached a settlement permitting the company to sell the list only to qualified buyers in the same general market as Toysmart.com who promised to abide by the original policy.[39] However, critics derided the agreement for not protecting customers,[40] and the bankruptcy court ultimately rejected the proposed settlement.[41]

The disposition of the list was eventually resolved when Disney purchased Toysmart.com[42] and destroyed the list under the supervision

---

36 See id at ¶¶ 19–20 (alleging that Toysmart.com had collected information about children without parental consent in violation of the Children's Online Privacy Protection Act, 15 USC § 6503 (2000)).

37 See id at ¶¶ 16–18 (alleging that Toysmart.com, by representing that it would never sell customer information, had engaged in a deceptive practice in violation of the Federal Trade Commission Act, 15 USC § 45(a)).

38 See Memorandum and Order on the State of Texas Motion to Intervene, *FTC v Toysmart.com, LLC*, 2000 US Dist LEXIS 21963 (D Mass). See also Objection of the Commonwealth of Massachusetts and 46 States to the Debtor's Motion to Approve Settlement with Federal Trade Commission and for Authority to Enter into Consent Agreement, *In re Toysmart.com* (Bankr D Mass filed Aug 10, 2000), available online at <http://www.naag.org/features/Final%20Opposition%20to%20FTC%20Settlement.pdf> (visited July 22, 2002) ("The States earlier filed an objection to the Debtor's proposed sale of its 'Customer List'" because "that sale would constitute an unfair or deceptive practice in violation of the Customer Protection Acts of the States.").

39 See Stipulated Consent Agreement and Final Order, *FTC v Toysmart.com*, Civil Action No 00-11341-RGS (D Mass July 21, 2000), available online at <http://www.ftc.gov/os/2000/07/toysmartconsent.htm> (visited June 12, 2002) (ordering that "absent approval by the Bankruptcy Court ... of the sale of the Customer Information to a Qualified Buyer or a reorganization plan, Defendants ... shall, on or before August 31, 2000, delete or destroy all Customer Information in their possession, custody or control," and defining "Qualified Buyer" as "an entity that (1) concentrates its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction, ... and (2) expressly agrees to the obligations set forth in the Stipulation and Order Establishing Conditions on Sale of Customer Information").

40 See, for example, Objection of the Commonwealth of Massachusetts and 46 States to the Debtor's Motion to Approve Settlement with Federal Trade Commission and for Authority to Enter Into Consent Agreement, *In re Toysmart.com* (filed Aug 10, 2000) (asserting that "the FTC proposes that Toysmart sell its customer list to a third party" and standing by its objection "that such a sale of the customer list to a third party is an unfair or deceptive actor practice").

41 See Order Denying Motions to Approve Stipulation with Federal Trade Commission and for Authority to Enter into Consent Agreement by Toysmart.com, *In re Toysmart.com* (filed Aug 17, 2000), available online at <http://pacer.mab.uscourts.gov/bc/cgi-bin/rundkt.pl> (visited June 26, 2002). One FTC commissioner who had voted against the settlement even went so far as to argue that no sale of the customer list should ever be permitted. See Federal Trade Commission, Dissenting Statement of Commissioner Orson Swindle, available online at <http://www.ftc.gov/os/2000/07/toysmartswindlestatement.htm> (visited Feb 5, 2002) ("Toysmart promised its customers that their personal information would *never* be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because 'never' really means never.").

42 Buena Vista Internet Group, a subsidiary of Disney, owned 60 percent of Toysmart.com

of the bankruptcy court.[43] The ramifications of the dispute, however, continued to spread throughout the online retailing industry. After *Toysmart.com*, several other companies experienced similar customer list problems. For instance, when Living.com, an online home furnishing retailer that had also posted a privacy policy on its site,[44] filed for bankruptcy, it avoided a court battle by reaching a settlement with the Texas attorney general. Under this settlement, Living.com agreed to sell only nonfinancial information about its customers.[45] Another bankruptcy settlement with Craftshop.com was concluded under similar constraints.[46]

This approach has had an important impact on the ability of online companies to use their most important asset: their customer lists. Although we may never know how many companies have been discouraged from selling their lists because of these statements, cases such as Living.com's and Craftshop.com's are clearly noticed by companies and consumers alike. Fry's Electronics's bid to buy Egghead.com is a good example. Fry's bid $10 million to buy Egghead.com and its customer list.[47] Before transferring the customer list, however, Egghead's customers were to be given an opportunity to "opt out"[48] and therefore not have their information transferred to Fry's. Because this might significantly dissipate the value of the asset it sought to purchase, Fry's conditioned the sale on no more than 10 per-

---

prior to the complete sale. See Brad Eric Scheler, *Bankruptcy Issues for High Tech Companies*, 1255 PLI/Corp 351, 369 (May/June 2001).

43 Stephanie Stoughton, *Toysmart.com List to Be Destroyed*, Boston Globe D7 (Jan 30, 2001) (reporting that the bankruptcy judge had approved the destruction of Toysmart.com's customer list).

44 See Office of the Texas Attorney General, Press Release, *Cornyn Announces Privacy Settlement with Living.com* (Sept 25, 2000), available online at <http://www.oag.state.tx.us/newspubs/releases/2000/20000925living.com.htm> (visited Feb 5, 2002) (noting that Living.com's privacy policy stated, "Living.com does not sell, trade or rent your personal information to others without your consent. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank email to never@living.com.").

45 Eisenbach, *Internet Company's Customer List* at 27 (cited in note 1) ("Living.com agreed to destroy its customer personal financial information but was permitted to transfer nonfinancial information only if customers did not opt-out after receiving a notice via email of a proposed transfer."). Texas Attorney General John Cornyn heralded the settlement by proclaiming: "It is important that Internet companies respect Texans' privacy rights whether the company is in the black—or in the red. This settlement will set the standard for future settlements and protect Texans' privacy rights." Office of the Texas Attorney General, Press Release, *Cornyn Announces* (cited in note 44).

46 See Marjorie Chertok and Warren E. Agin, *Restart.com: Identifying, Securing and Maximizing the Liquidation Value of Cyber-Assets in Bankruptcy Proceedings*, 8 Am Bankr Inst L Rev 255, 302 (2000) (describing how, in order to use its customer list, the purchaser of bankrupt Craftshop.com was required to continue the use of the Craftshop name).

47 Troy Wolverton, *Egghead Sale Could Crack on Privacy Issues*, News.com (Aug 24, 2001), available online at <http://news.com.com/2100-1017-272130.html> (visited July 22, 2002).

48 Id. An opt-out policy generally requires that a letter be sent to the customer requesting a reply if he does *not* want his information transferred to a third party. See id.

cent of Egghead.com's active customers opting out.[49] Eventually the deal fell through and Amazon.com agreed to buy Egghead.com for $6.1 million[50] and abide by email spamming constraints.[51] At a minimum, therefore, the restrictions on selling customer lists have made deals involving customer lists more expensive and have resulted in a lower return for companies trying to sell their customer lists. Yet, the impact could go far beyond this if companies are discouraged from creating lists altogether or are destroying their lists for fear that attempting to sell them will generate bad press or lessen their ability to sell their other assets.

D. Legislative Proposals

Outside the bankruptcy court, legislators have also attempted to address online privacy concerns. For instance, bills have been introduced recently to prohibit online companies from selling their lists after filing for bankruptcy.[52] Other proposed bills would regulate the use of online information, either gathered or sold.[53] Although the various

---

49 See id (quoting an intellectual property lawyer as reasoning that since "the 10 percent figure is so low, it indicates that the customer list is the main asset that Fry's cares about," and estimating that the list consisted of 4 million customers, 1.3 million of whom were "active").

50 Mark Franco, *Mergers & Acquisitions: Few Wanted to Make a 4Q Deal*, Catalog Age (Mar 1, 2002), available online at <http://catalogagemag.com/ar/marketing_mergers_acquisitions_few/index.htm> (visited July 22, 2002).

51 Bob Liu, *Egghead.com Becomes Amazon.com Property*, Seattle Internet News (Dec 3, 2001), available online at <http://www.internetnews.com/bus-news/article.php/3_932871> (visited July 22, 2002).

52 See Bankruptcy Reform Act of 2001 § 231, S 420, 107th Cong, 1st Sess (Mar 1, 2001) (passed Senate, passed House as HR 333, engrossed in Committee) (amendment aimed at protection of nonpublic personal information); Privacy Policy Enforcement in Bankruptcy Act of 2000, S 2857, 106th Cong, 2d Sess (July 12, 2000) (engrossed in Senate) (a bill to exclude personally identifiable information from the assets of a debtor in bankruptcy). While these changes to the bankruptcy code have been proposed to solve this problem, they would likely only create more confusion. Companies that previously would have filed for bankruptcy may instead attempt to sell the list outside bankruptcy or sell the company in its entirety, thereby transferring the list without involving the prohibitions likely to be placed on them if the changes to the bankruptcy code are accepted). See Paul Davidson, *Hot Commodity: Dot-com Lists: Creditors' Asset of Choice*, Natl Post E02 (Mar 5, 2001) (citing research conducted by a Webmergers.com study, which found that at least 95 e-tailors failed in 2000 "and many did not file for bankruptcy court protection"). See also Steven D. Homan, *Attorneys and Wall Street Deal with the Dot-Com Downturn*, NY L J 5 (Aug 9, 2000) (questioning whether new economy companies should seek bankruptcy protection at all). Companies such as eToys have managed to avoid bankruptcy issues by bundling their customer lists for sale with the company as a whole. See Arlene Weintraub, *E-Assets for Sale—Dirt Cheap*, Business Week EB20 (May 14, 2001) (discussing e-tailer liquidation options and noting that "eToys says it won't sell its customer information, unless somebody buys the whole company").

53 See, for example, HR 4814, 106th Cong, 2d Sess (July 10, 2000) (referred to House Committee on Commerce) (amending Section 5 of the Federal Trade Commission Act to make it unlawful "for a person to sell on the Internet information such person acquired with a pledge that the information would be kept private and not released or for a person to share or transfer to another such information on the Internet"). See also Consumer Internet Privacy Enhance-

bills address a wide variety of activities, the proposals are similar in that they focus almost exclusively on the Internet.

The proposals consistently reflect the belief that the Internet requires new rules and a new standard when it comes to customer privacy. For instance, the Consumer Internet Privacy Enhancement Act[54] prohibits a "commercial website operator [from collecting] personally identifiable information online from a user of that website unless the operator provides (1) notice to the user . . . and (2) an opportunity to that user to limit the use" of the personal information.[55] Senator John McCain, one of the Act's cosponsors, introduced the bill by distinguishing between Internet and traditional commerce.[56] Although he acknowledged that "[s]ince the beginning of commerce, business has sought to learn more about customers," he claimed that the "[t]he ability of the internet to [collect and use such information] about a consumer's habits is unprecedented."[57] Another cosponsor, Senator John Kerry, compared online and offline privacy and concluded that the threat is significantly greater online.[58] While the Act actually proposed allocating money for studying the relationship between online and offline privacy,[59] all the specific prohibitions in the Act applied only to online industries.

This Part has demonstrated how courts, commentators, and legislators have treated online and offline companies' customer lists differently. The legal distinction must be founded, if at all, on some important difference between offline and online companies' use or sale of customer lists. Maybe the law is attempting to address different customer concerns between online and offline companies, or perhaps the developed law for offline companies is inadequate to cover online companies. In fact, neither is the case. In the next Part, I demonstrate that the concerns of offline companies' customers are nearly identical to those of online companies' customers.

---

ment Act, S 2928, 106th Cong, 2d Sess (July 26, 2000) (prohibiting a commercial website operator from collecting personally identifiable information online from a user unless the operator notifies the user or gives user an opportunity to limit its use).

54 Consumer Internet Privacy Enhancement Act, S 2928, 106th Cong, 2d Sess (July 26, 2000).

55 See id.

56 Id.

57 Id.

58 See id. Senator Kerry was particularly concerned about the loss of anonymity online that results from being able to track consumers when they are only browsing.

59 Id at § 5(b)(3) (authorizing the National Resource Council to "examine the differences, if any, between the collection and use of personal information by the online industry and . . . by other business").

II. EXISTING CASE LAW ON CUSTOMER LISTS

For those who have followed the bankruptcies of online companies and the subsequent fights over their customer lists, these issues may seem like a new frontier. The vast majority of debate surrounding customer lists either ignores offline precedent or treats it as inapplicable to the current debate.[60] Interestingly, while online companies' desire to sell their customer lists could have been addressed solely through traditional contract law, commentators have instead chosen to confront the issues by referencing privacy rights in personal information.[61] A common misconception exists that customer lists are new inventions. In fact, references to customer lists have appeared regularly in case and statutory law for almost three decades.[62] This Part will take a step back from the recent privacy rhetoric and provide a survey of customer list precedent.

Courts often treat offline customer list cases without discussing privacy at all. Instead, courts routinely treat offline customer lists simply as corporate property. When courts do discuss the privacy concerns of offline customer lists, however, they often rule against consumers who argue that companies use the lists to violate privacy. This Part discusses the various ways offline customer lists have been viewed in case law. In general, the case law arises in one of three broad categories: (1) customer lists as trade secrets of a corporation; (2) customer lists claimed as property of a corporation; and (3) customer lists as the objects of privacy claims against companies that collect or use the lists.

A. Customer Lists as Trade Secrets

Courts most often discuss customer lists in regard to their status as trade secrets.[63] Courts have repeatedly found that customer lists

---

60 See, for example, Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan L Rev 1125, 1131, 1159–69 (2000) (acknowledging that "the law does not generally recognize the legal right of individuals to control uses or disclosures of personal data," but focusing almost exclusively on cyberspace information privacy problems). See also Penn, 2000 ABI J Lexis 81 at *6 (cited in note 1) (noting that the privacy debate ignores precedent).

61 See Office of the Texas Attorney General, Press Release, *Cornyn Announces* (cited in note 44). See also Walter W. Miller, Jr., and Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 Houston L Rev 777, 848 (2001) (advocating a regulatory approach based upon privacy rights).

62 See, for example, *Dwyer v American Express Co*, 273 Ill App 3d 742, 652 NE2d 1351 (1995); Eisenbach, 18 Computer & Internet Law at 25 (cited in note 1); Penn, *Internet Privacy*, 2000 ABI J Lexis 81 at *6 (cited in note 1).

63 See, for example, *Defiance Button Machine Co v C & C Metal Products Corp*, 759 F2d 1053, 1063 (2d Cir 1985) (holding that the customer list in question was not a trade secret, but noting that "[a] customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret and protected at the owner's instance against disclosure to a competitor, provided the information it contains is not otherwise readily ascertainable");

qualify as trade secrets as long as such rulings do not interfere with the basic tenets of state law.[64] These cases often have nothing to do with the Internet and never mention the "rights" of third parties (in other words, the customers themselves) to the customer information. In fact, courts routinely treat customer lists as property under trade secret law without any additional discussion of the rights of customers—even while the Internet privacy debate rages about them.[65] This is not just judge-made law; several states have statutes explicitly recognizing customer lists as viable trade secrets.[66] Treating a customer list as a trade secret affirms corporations' property interests in such lists. Furthermore, lists that are considered trade secrets are considered freely alienable, much as trade secrets are in general.

B. Customer Lists as Corporate Property

Aside from considering customer lists to be trade secrets, courts also explicitly treat customer lists as exclusively corporate property. For instance, in *Miller v Ortman*,[67] the Indiana Supreme Court held that a customer list was a part of "the good will of a business" and therefore protected under contract principles.[68] As part of goodwill, the customer list is freely alienable and owned by the corporation. Furthermore, *Miller* can be read as providing an incentive for companies to invest in collecting customer lists in the first place.

Nearly twenty years later, the Seventh Circuit in *In re Uniservices*[69] referred to *Miller* approvingly and added that the fact that the company's "customer information constitutes protectable property is

---

Avery Dennison Corp v Kitsonas, 118 F Supp 2d 848, 854 (S D Ohio 2000) (holding that a customer list is "a trade secret under Ohio law as it is: 'business information or plans, financial information or listing of names, addresses or telephone numbers'"), citing Ohio Uniform Trade Secrets Act, Ohio Rev Code Ann § 1331.61; *Heritage Benefit Consultants v Cole*, 2001 Conn Super LEXIS 543, *19 (holding that a customer list is a trade secret, which is defined under Connecticut law to include "information, including a compilation, program, . . . cost data or customer list"), citing Connecticut Uniform Trade Secrets Act, Conn Gen Stat § 35 et seq; *Hayes-Albion v Kuberski*, 311 NW2d 122, 127 (Mich App 1981) (confirming the trial court's holding that the plaintiff's customer list was a trade secret).

64 See, for example, *Avery Dennison*, 118 F Supp 2d at 854; Miller and O'Rourke, 38 Houston L Rev at 787–88 (cited in note 61) ("That the law often accords customer lists property-type rights is evident by the number of cases holding them to be trade secrets.").

65 Note that the cases cited in note 63 arose between 1981 to 2001, spanning the development of the Internet.

66 See, for example, Conn Gen Stat Ann § 35-51(d) (West 2001) ("'[T]rade secret' means information, including a . . . customer list.").

67 235 Ind 641, 136 NE2d 17 (1956).

68 Id at 34 ("Public policy is committed to the proposition that a man is free to conduct a lawful business and that good will of a business . . . such as the names and addresses and requirements of customers . . . is a property right which an owner is entitled to protect.").

69 517 F2d 492 (7th Cir 1975). See also *Frank v Hadesman and Frank Inc*, 83 F3d 158, 161 (7th Cir 1996) ("A customer list is property of the firm, and an employee . . . who puts that information to personal use has violated a duty to the corporation.").

underscored by the assignment thereto of independent market values."[70] Rather than examining a customer's right to the information contained in the customer lists, these cases treated the customer list as corporate property that is both valuable and freely alienable.

More recent cases have not strayed from these cases' analysis or their conclusions. For example, *In re Andrews*[71] involved a bankrupt debtor who had sold his customer list as part of a pre-petition sale.[72] The list sold for approximately $1 million and the validity of the sale was not questioned.[73]

Another bankruptcy case, this one from 1997—well into the Internet era[74]—addressed the valuation of a customer list.[75] Once again, the court focused on a correct valuation of the list itself for the purposes of sale rather than discussing the privacy rights of the customers on the list.[76]

Other cases have permitted debtors to grant security interests in customer lists, thereby acknowledging the debtors' property interest in those lists and allowing the sale of the customer lists in the normal course of business.[77] In addition, statutes and commentators recognize that customer lists are treated as assets that a company buys and sells.[78] Notably absent from these discussions, however, is any discussion of privacy issues or the rights of customers to retain an interest in the personal information contained in the lists. By emphasizing the companies' ability to grant alienable security interests, courts appear to

---

70 *Uniservices*, 517 F2d at 496.

71 80 F3d 906 (4th Cir 1996).

72 Id at 908.

73 See id. The court does not address the validity of the sale and treats it as unproblematic. While this silence is not dispositive, it does suggest that the sale of the list was not controversial and that the list was considered property of the estate.

74 According to some estimates, there were over 50 million Internet users over the age of sixteen in the U.S. and Canada in 1997. See CommerceNet, *Industry Statistics: Internet Population*, available online at <http://www.commerce.net/research/stats/wwwpop.html> (visited June 12, 2002).

75 See *In re Lifschultz Fast Freight*, 132 F3d 339, 352 n 12 (7th Cir 1997).

76 See id:

> The fact is that the debtor's list was generating $22 million a year in revenue. Even if the debtor could not make money with it, maybe somebody else could. The debtor's customers were a premium bunch: all were willing to pay high prices for good service, and the list manifested that information.

77 See, for example, *In re Roman Cleanser Co*, 802 F2d 207, 208 (6th Cir 1986) (recognizing an interest in a trademark and the associated goodwill, including a customer list).

78 See, for example, Internal Revenue Code, 26 USC § 936(h)(3)(B)(v) (1994) (defining "intangible property" from which income can be derived as including a "customer list"). Consider also Steven L. Kroleski and David R. Rant, *Use of Customer Lists: A Unified Code Is the Solution*, 15 Westchester Bus J 189, 209 ("All lists should be considered assets of the employer, as evidenced by the fact that, when a business is sold, monies are paid for such assets.").

believe that offline lists do not present any privacy concerns for consumers.

C. Privacy Issues

Even when courts discuss the privacy issues surrounding offline customer lists, they conclude that privacy concerns are not sufficient to restrict the sale of these lists.[79] Offline cases, therefore, while discussing the effect of customer lists on consumer privacy rights, nevertheless uphold lists' alienability.

For instance, courts have repeatedly upheld the right of companies to collect and sell personal information about their customers despite the customers' protests that such sales invaded their right to privacy. In 1975, an Ohio Appeals Court upheld the right of American Express to gather and sell customer information, as well as the right of magazine publishers to solicit customers based on this data.[80] The plaintiffs alleged that the defendant's practice of renting and selling subscription lists constituted an invasion of privacy and unjust enrichment.[81] In allegations that are remarkably similar to those espoused by modern privacy advocates,[82] the plaintiffs contended that customer lists invade their privacy by enabling others to "draw certain conclusions about [their] financial position [and] social habits."[83] The plaintiffs further argued that the magazine publishers had invaded their privacy by using customer lists to mail specially targeted advertisements to the plaintiff's homes.[84] The court dismissed both these allegations and held that the defendants' practices did not infringe on any constitutionally protected right to privacy.[85]

Another example of judicial refusal to recognize customer privacy concerns may be found in the general practice of allowing a state department of motor vehicles to sell personal information gathered from drivers. Currently, several states permit their department of motor vehicles to sell personal information gathered from drivers.[86] *La-*

---

79 See Parts II.A and II.B.

80 *Shibley v Time, Inc*, 45 Ohio App 2d 69, 341 NE2d 337, 340 (1975).

81 See id at 338.

82 See Part I.C.

83 *Shibley*, 341 NE2d at 339.

84 See id.

85 See id ("[T]he right of privacy does not extend to the mailbox and therefore it is constitutionally permissible to sell subscription lists to direct mail advertisers.").

86 See, for example, Illinois Vehicle Code, 625 ILCS 5/2-123 (West 2001) (authorizing the secretary of state of Illinois to sell drivers' personal information to select government officials and agencies). But see *Reno v Condon*, 528 US 141, 151 (2000) (upholding the Driver's Privacy Protection Act of 1994, which restricts the ability of states to distribute drivers' personal information); Driver's Privacy Protection Act of 1994, Pub L No 103-322, 108 Stat 2099, codified at 18 USC §§ 2721–25 (1994 & Supp 1998) (regulating the disclosure of personal information contained in the records of state motor vehicle departments).

mont v Commissioner of Motor Vehicles[87] addressed the right of the State of New York to sell information it had received through the compulsory registration of its citizens at the department of motor vehicles.[88] Although the DMV distributed information to businesses who then used it to direct advertising to certain residents, the court dismissed the case and explained: "The mail box ... is hardly the kind of enclave that requires constitutional defense to protect 'the privacies of life.' The short, though regular, journey from mail box to trash can ... is an acceptable burden."[89]

As both *Shibley* and *Lamont* demonstrate, courts considering the practice of collecting and selling customer lists have generally rejected customers' privacy claims. Given this precedent, why has online privacy become such an important issue? Have sensibilities changed, so that we are more concerned with privacy now than we were before? Or is there something unique about the Internet context that makes us more concerned with privacy rights in cyberspace?

At least some cases suggest that the courts, if not the public, are no more concerned with customer privacy in the traditional business context now than they were fifty years ago. *Dwyer v American Express Co*,[90] decided in 1995, suggests that non-Internet companies continue to be treated in line with earlier precedent. *Dwyer* is remarkably similar to *Shibley*, both in the claims presented and its holding. The plaintiffs in *Dwyer* alleged that American Express had gathered and sold customer information, thereby invading their privacy. Relying primarily on *Shibley* and *Lamont*, the court dismissed the claims and noted that such privacy concerns were unfounded: "[D]efendants' practices do not deprive any of the cardholders of any value their individual names may possess."[91] As the *Dwyer* opinion indicates, technology may have developed significantly since *Shibley*, but the non-Internet world has remained remarkably stable.

III. THE TECHNOLOGY SPLIT IS UNWARRANTED

If the Internet has changed data collection to the extent that collecting personal information about consumers now presents entirely different legal issues, a change in the underlying law may be justified. For instance, if the online data is more susceptible to abuse or more intrusive than offline data, it may be appropriate to have different

---

87 269 F Supp 880 (S D NY 1967).

88 See id at 882.

89 Id at 883.

90 273 Ill App 3d 742, 652 NE2d 1351, 1357 (1995) (noting that the only damage plaintiffs suffered as a result of the release of their personal information to other companies was a "surfeit of unwanted mail").

91 Id at 1356.

rules for online and offline companies. On the other hand, if the only difference lies in the medium by which the information is gathered and disseminated, then any distinction between them would be unjustified. This Part compares the collection of customer lists across media and concludes that any differences that exist are not significant enough to justify establishing different legal standards for Internet companies.

A. How Different Is the Information Gathered from the Internet?

Contrary to popular opinion,[92] it is not at all clear that significantly more valuable or sensitive information is gathered online. Many companies that provide the data collection capabilities about which commentators have warned either do so without a personal identifier, or have since shut down because of the tremendous costs associated with collecting the data.[93]

Furthermore, it is not clear that the data collected by Internet companies is any more intrusive than that collected by other businesses. Consider the following two sets of data that have been compiled by businesses doing customer research:

> Set 1: Lists that analyze where customers shop, how much they spend, their behavioral characteristics, and spending history. The lists further categorize customers into groups such as "mail-order apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers."[94]

> Set 2: Lists that include "name, address, billing information, shopping preferences, and family profiles, which include the names and birth dates of children."[95]

It is difficult to detect significant differences between the two sets of information or determine which set is more offensive or intrusive to a

---

92 See, for example, Michael Sonsino, *U Pennsylvania: Study Addresses Customer Concerns About Online Privacy, Safety*, U-Wire, 2000 WL 26933934 (Sept 19, 2000) (reporting that concerns about privacy and security hamper Internet shopping). See also Koster, 16 No 5 Computer Law at 7 (cited in note 17) (arguing that the Internet has influenced privacy issues by reducing the cost of information and by increasing the value of such information by improving the ability of companies to link data and thus better target potential customers).

93 See Stephanie Miles, *DoubleClick Halts Service That Targets Ads to Web Surfers*, Wall St J B6 (Jan 10, 2002) (describing how Doubleclick, an online advertising firm, dropped a service that targeted advertisements at individual behavior based on data collected about where that user had gone on the Web).

94 *Dwyer*, 652 NE2d at 1353 (describing the types of lists generated by American Express to categorize and rank its cardholders).

95 Federal Trade Commission, Press Release, *FTC Sues* (cited in note 12).

customer. Although information about children may be of special concern, and therefore require additional legislation, there is no reason to think that the information collected online about children will be significantly different from that garnered offline. Most would probably conclude that they are similar, and that any differences are negligible. The first set, however, was collected offline by a credit card company[96] and later determined to be freely alienable.[97] The second set is an example of data collected by Toysmart.com.[98] Although the two sets of data appear similar, a court restricted the sale of the second set of data to third parties.[99] Furthermore, the FTC's lawsuits and settlements, as well as the numerous legislative proposals and academic articles, have only been directed toward online companies like Toysmart.com.[100]

B. The "Other Side" of Technology

For a moment, assume that Internet companies can use technology to gather intrusive information about their customers more effectively. Even if this is true, any conclusions about the new technology's impact on privacy must account for the fact that technology is not one-dimensional. The same advances in technology that companies use to gather information for marketing can also be used to protect customers from misuse of that information.

Several companies have developed new products to respond to the demand for online privacy.[101] These products not only make it easier for a user to conceal her identity while shopping or web surfing,[102] but they also enable her to avoid harassing emails and phone calls from marketing organizations.[103]

Moreover, most email systems employ various filters that screen out unwanted junk mail.[104] Even if spam manages to pass through the

---

96 See *Dwyer*, 652 NE2d at 1353.

97 Id at 1356 (denying the plaintiffs' claim of invasion of privacy and consumer fraud and thereby permitting the sale of customer lists).

98 See Federal Trade Commission, Press Release, *FTC Sues* (cited in note 12).

99 See Part I.C.

100 See id.

101 See, for example, the TeleZapper home page, available online at <http://www.telezapper.com> (visited Feb 4, 2002) (advertising the "TeleZapper" as a product that automatically removes customer phone numbers from telemarketers' databases). See also <http://www.epic.org/privacy/tools.htm> (visited Feb 4, 2002) (listing and making available for download several software tools for customers who are concerned about Internet privacy).

102 See McGeveran, 76 NYU L Rev at 1826–33 (cited in note 27) (describing how P3P, an innovative "privacy-enhancing technology," operates to protect the privacy of online users).

103 The producers of the TeleZapper, for instance, claim their product will remove customer phone numbers from databases that are purchased and used by telemarketers. Removing the phone numbers will therefore decrease the likelihood of receiving a telemarketers' call. See <http:www.telezapper.com/faq.htm> (visited Aug 5, 2002).

104 For example, Yahoo! Mail allows users to direct mail to different folders depending on the sender or the subject title. See <http://mail.yahoo.com> (visited June 3, 2002).

various filters, today's technology makes it easy to delete it with just a few clicks.[105] Nearly thirty years ago, *Lamont* ruled that junk mail did not infringe on a person's right to privacy.[106] Surely the change in technology has not made the trip to the "mailbox" any more "noxious." On the contrary, given that it has become even easier to "take out the trash," it is difficult to criticize unwanted junk mail as an intolerable infringement on individual rights, even though the volume of such mail may have increased substantially.

C. Technology's Privacy-Enhancing Capabilities

Some argue that limiting the sale of customer lists—or prohibiting their sale altogether—would do much to benefit customers.[107] However, customer lists often enable web companies to offer their services for free or, at a minimum, for sharply reduced prices.[108] Websites that want to attract visitors often must allow significant access for free.[109] By collecting information about their visitors, and then selling it to other companies, the online companies can stay in business while providing a free service to a wide audience.[110]

Advances in technology have enabled Internet companies to compile customer lists that can presumably be more detailed.[111] Thus, such lists can be used as a means to develop more personalized marketing. Rather than becoming *more* intrusive, online companies may become *less* intrusive because more accurate and focused advertising may actually mean customers endure fewer unwanted contacts from companies' marketing departments.[112] In fact, a survey conducted by *Privacy & American Business*[113] suggests just how valuable customer lists—or at least the uses of such lists—can be to the customers themselves. The survey found that most customers prefer receiving banner

---

105 Deleting mail on Yahoo! or Microsoft Outlook requires only selecting the message(s) and clicking the "delete" button.

106 *Lamont*, 269 F Supp at 883 (claiming that a trip to the mail box "is an acceptable burden").

107 See generally Miller and O'Rourke, 38 Houston L Rev 777 (cited in note 61).

108 See Hetcher, 7 Mich Telecomm & Tech L Rev at 130 (cited in note 4) (explaining how online companies use data collection and processing as sources of revenue, which in turn allows them to offer websites for free).

109 See id.

110 See id.

111 See Koster, *Zero Privacy* at 7 (cited in note 17) ("The Internet has both facilitated the gathering of personal data and, by improving the ability to link vast amounts of data to a particular individual, made the data more valuable.").

112 But see Federal Trade Commission, *Privacy Online: Fair Information Practices* at 2–3 (cited in note 22) (stressing that privacy concerns likely have limited the growth of the online marketplace).

113 *Privacy & American Business, Executive Summary* (July 1999), available online at <http://www.pandab.org/doubleclicksummary.html> (visited Feb 4, 2002) (asking a sample of Internet users a series of questions about online personalized marketing).

advertisements tailored to their personal interests.[114] Furthermore, it found that more than two-thirds of Internet users would willingly provide personal information in order to receive tailored ads.[115]

By providing personal information, the consumer can receive more targeted solicitations and fewer advertisements in which she has no interest. This reduces the amount of time she must spend searching for the right products and services, and also decreases the time spent disposing of superfluous offers. The company, on the other hand, gains because it no longer has to spend money sending offers to individuals who are not interested in its products, but can use its resources to market to a select group who will be more likely to make a purchase. Therefore, courts that place restrictions on the collection and sale of customer lists should be careful to take these costs into account. Courts need to recognize that the more tailored the customer list is to the customer, the more valuable it will be to the company and to the customers themselves.

D. There Is No Such Thing as an Online Company

So far, this Comment has assumed that online companies are distinguishable from offline companies. The Comment has adopted this assumption only because it is reflected in the *Toysmart.com* litigation,[116] in academic literature,[117] and in major legislative proposals.[118] The assumption, however, is false. There is no clear demarcation between online and offline companies or their respective customer information.

---

114 See id ("A majority of Internet users (61 percent) say they would be positive toward receiving banner ads tailored to their personal interests rather than receiving random ads.").

115 Id ("More than two-thirds of Internet users (68 percent) say they would provide personal information in order to receive tailored banner ads, if notice and opt out are provided.").

116 See, for example, Federal Trade Commission, Statement of Commissioner Mozelle W. Thompson, available online at <http://www.ftc.gov/os/2000/07/toysamrtthompsonstatement.htm> (visited Feb 4, 2002) ("This case is important because it directly considers the obligation of an *online business* to its customers.") (emphasis added). See also Federal Trade Commission, Press Release, *FTC Sues* (cited in note 12) ("Even failing dot-coms must abide by their promise to protect the privacy rights of their customers."), quoting FTC Chairman Robert Pitofsky.

117 See Federal Trade Commission, *Privacy Online: A Report* at 40 (cited in note 5):

> While American businesses have always collected some information from customers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises customer concerns.

See also id at 2 ("The World Wide Web is an exciting *new* marketplace for customers.") (emphasis added).

118 See Part I.D.

For instance, a firm like Disney has a large web presence, with sites such as ESPN.com, ABCnews.com, and Disney.com.[119] Yet, it obviously also has a significant traditional, offline business.[120] It is impossible to separate the two lines of business. Data flows throughout an entire business and customers interact, not simply with a website, but with all of the company's operations. For instance, on the Disney.com site, visitors can buy tickets to the Disney theme parks or, in just two clicks, get to the home page for ABC.[121] The futility of distinguishing companies merely by the channel through which they provide services is likely to increase as companies become more sophisticated in their use of information and more adept at integrating their websites with their primary businesses.

Multimedia conglomerates are not the only companies for which classification between online and offline is difficult. Even the most traditional companies have blurred the distinction. For example, manufacturers of ball bearings offer a significant amount of information over their websites and even permit customers to purchase their products online.[122] Since the customer order is placed online, it is unclear whether this information would be subject to the online or the offline standard. Similarly, online companies have offices and physical facilities where they conduct business. E*Trade, one of the most prominent Internet brokerages, has financial centers located in New York, San Francisco, and Boston.[123]

IV. THE NEGATIVE CONSEQUENCES OF THE TECHNOLOGY SPLIT

Treating customer lists differently for online and offline companies is not simply harmless error. The technology split has serious, negative ramifications for both companies and customers. For instance, applying separate standards for companies creates inconsistent laws. Separate standards are also counter-productive because they create incentives for companies to change their structure in order to avoid the distinction altogether. Furthermore, the distinction punishes small online companies and encourages companies to have larger, more diversified businesses. This Part examines the consequences of treating online and offline customer lists differently.

---

119 See <http://www.espn.com> (visited Oct 12, 2002); <http://www.disney.com> (visited Oct 12, 2002); <http://www.abcnews.com> (visited Oct 12, 2002). All three sites are owned by the Disney Corporation and operated as part of the "Go" network.

120 ESPN, ABC and Disney all operate television networks as well as other offline ventures.

121 See <http://www.disney.com> (visited June 25, 2002).

122 See, for example, <http://www.emersonbearing.com> (visited June 12, 2002).

123 See, for example, <https://www.etrade.com> (visited June 12, 2002). They also operate more than 11,000 ATMs. <https://bank.etrade.com/access/locator.cfm> (visited June 12, 2002).

Large companies are, by definition, more likely to have greater resources that can be used to gather information about more customers. The larger the company, on average, the more money it can devote to marketing so that it can solicit customers for future business. Smaller companies will have fewer points of interaction with their customers and therefore will probably collect less detailed information about each customer.[124] Consequently, any policy that systematically favors larger companies will be counterproductive and will likely cause companies to consolidate and grow in order to capture that advantage.

The distinction between online and offline companies is an example of a policy that benefits large companies. Large companies derive their advantage from a loose interpretation of the term "third party." The term is typically used by website disclosure policies[125] and also serves as the foundation for legislation.[126] However, courts have yet to provide a clear definition of the term.[127] One stumbling point is that "third party" can mean something very different to a company than it does to that company's customers. Is ABC News a third party with respect to ESPN?[128] Most customers would probably think so, while Disney almost surely would not. Because the term "third party" remains vague, a company's assurance that it will not sell information to third parties may be a very empty and misleading promise.[129]

Regardless of how the meaning of the term is eventually resolved, the result will almost surely favor companies with larger, more diversified activities over smaller start-ups. To better illustrate this point, imagine two companies that sell educational games to children. Both companies have relatively similar websites and, consequently,

---

124 While there are certainly exceptions, larger companies tend to have larger web presences than their smaller competitors in the same industry. Furthermore, large companies may be better able to encourage their offline customers to transact business online and therefore leverage their size for their online business.

125 Most website policies state that they will not share information with "third parties." See Federal Trade Commission, *Privacy Online* at 20 (cited in note 5) (noting that a common "Privacy Policy Notice" often includes a statement promising that personal information will not be shared with third parties). See, for example, *EBay Says It May Sell Information on Users in Event of Acquisition*, Wall St J B7 (Apr 3, 2001) (noting that Toysmart posted a privacy statement on its website promising "not to turn private customer information over to third parties").

126 For example, S 2928 permits the collection of information when the site provides notice. Notice is defined as "a statement [identifying] the operator of the website and of any *third party* the operator knowingly permits to collect" information (emphasis added).

127 See Chertok and Agin, 8 Am Bankr Inst L Rev at 302–03 (cited in note 46) (discussing how the bankruptcy courts crafted various resolutions to the "third party" issue in determining whether purchasers of a debtor company may access that company's customer lists).

128 See text accompanying notes 119–20.

129 See Part I.C. See also Chertok and Agin, 8 Am Bankr Inst L Rev at 302–03 (cited in note 46) (noting how several companies have gotten around conditions on the sale of customers lists by creatively interpreting the term "third party").

similar customer lists. One of the websites, Subsidiary.com, is operated by a large, multi-national conglomerate, BehemothCorp, that also owns children's television programming, news stations, and numerous hard copy publications, intended for both children and adults. The other website, MiniCorp.com, is owned by a start-up company run by several young entrepreneurs who have no source of income other than venture capital funding. These companies are in competition with one another, and both have privacy policies guaranteeing that they will not sell customer information to "third parties."

What happens when the companies need to generate additional cash flow? One option is to run back and get more financing, either from its parent corporation (as Subsidiary.com would) or from its venture group (as MiniCorp.com would). Another option is to use the customer information that is collected on their websites, but still follow the privacy policies by not sharing information with third parties. Subsidiary.com could almost certainly share its customer information with the other divisions of BehemothCorp, such as its magazine division, or use it to generate marketing opportunities for its children's television shows. All of these companies belong to the same corporate family that initially collected the information and therefore fall outside the loose definition of "third party." This, in turn, could encourage BehemothCorp to fund the website of Subsidiary.com. If there are restrictions on the alienability of customer lists, such as an inability to sell to third parties, MiniCorp.com has no other options. It cannot sell or lease the information to others who might value the customer list. Although MiniCorp.com will have invested just as much in its customer list, it will reap significantly less return on its investment than Subsidiary.com.

A company that cannot sell its customer list will also be at a disadvantage when attempting to obtain financing or generate cash flow. Prospective investors in MiniCorp.com, discouraged by a lower rate of return than the equivalent Subsidiary.com, as well as the likelihood of a court battle over the customer information in the event of a bankruptcy filing,[130] will charge a higher price for their dollars or choose to invest in the beneficiary of the loose "third party" definition—BehemothCorp. Furthermore, even if MiniCorp.com were able to obtain financing, its inability to sell its customer list, or share the list across divisions like Subsidiary.com, means that it will have lower earnings and cash flow. These factors may be enough to give a permanent competitive edge to Subsidiary.com.

If MiniCorp.com goes out of business, it not only harms the company and its creditors, it harms consumers as well. Strict customer list

---

130 See Part I.C.

laws reduce the ability for small companies to compete, thereby reducing choice for consumers and increasing costs. The laws would not have the same effect on Subsidiary.com. For instance, when Disney destroyed Toysmart.com's customer list, it probably did not suffer any significant loss; it likely had a remarkably thorough list of similarly situated customers.[131]

As this illustration demonstrates, large companies enjoy substantial benefits from a loose definition of "third parties." Unsurprisingly, therefore, the FTC has noted that large companies have been much quicker to adopt privacy policies.[132] In addition to any benevolent intentions and smart public policy rationales, these companies may have recognized their comparative advantage over smaller companies. A larger company would look more attractive to the customer because of its privacy policy, but it has actually lost almost nothing by posting such a policy. Because of the loose definition of third parties, the large company with a privacy policy has not totally eliminated its ability to alienate its customer lists. Although the Internet has been touted as a great equalizer[133]—a market where the "little guy" can effectively compete against the conglomerates[134]—restrictions on the alienability of customer lists may be one way the large companies can maintain their dominance in the market.

The most telling sign that large companies recognize this advantage is that, even when small companies try to avoid restrictive disclosure policies, large companies take it upon themselves to restrict the dissemination of customer information.[135] Several large companies now require that small companies comply with privacy guidelines in order to advertise on their sites or otherwise take advantage of their services.[136]

---

131 Disney owned 60 percent of Toysmart.com and probably had a relatively similar customer base. Scheler, 1255 PLI/Corp at 369 (cited in note 42).

132 See Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* 12–13 (July 1999), available online at <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (visited June 12, 2002) ("Companies like IBM, Microsoft and Disney, which have recently announced, among other things, that they will forgo advertising on sites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues."). Compare Saul Hansell, *Privacy Policy on Web Shifts as Profits Ebb*, NY Times A1 (Apr 11, 2002) (noting that Yahoo! and Excite are changing privacy policies and seeking to sell their customer lists).

133 See Tim Padgett, *The Net Heads South (to Latin America)*, Time B14 (Oct 8, 2001).

134 See id.

135 Large companies may also be restricting the dissemination of information in order to avoid more restrictive governmental policies. However, this Comment points out that it is also clearly in their interest to do so in order to gain an advantage over small companies.

136 Federal Trade Commission, *Self-Regulation* at 12–13 (cited in note 132). See also Hetcher, 7 Mich Telecomm & Tech L Rev 97 at 142–43 (cited in note 4):

> [L]arge sites devised a means to bring small sites into conformity with more respectful data collection practices. Large sites began threatening to withhold advertising from sites that

A final complication for courts is that, since there is no important difference between online and offline companies or data,[137] the supposed distinction between these types of customer lists can be described as, at best, arbitrary or overinclusive. If courts were to hold that laws restricting the alienability of customer lists applied to all information collected or distributed online, the law could theoretically apply to every company. If the law applies to all companies, it risks violating established precedent.[138] On the other hand, if courts drew a distinction between online and offline companies, this distinction would necessarily be arbitrary and would create unnecessary complexity, cost and confusion. For instance, parties in a privacy dispute would have to argue that the company, or the information it collects, should be classified as online or offline—thereby increasing litigation costs and creating uncertainty for businesses when they attempt to sell customer lists or use them as collateral for raising capital.[139]

This Part has described how applying a different standard to online and offline companies is counterproductive because it helps large companies at the expense of smaller ones. The distinction actually benefits those companies that are most likely to engage in mass solicitation and marketing campaigns. Large companies are also most likely to be able to avoid the impact of privacy policies altogether by broadly interpreting laws and disclosure policies. Small companies, on the other hand, will either be harmed by their inability to transfer customer lists or will attempt to avoid having a privacy policy altogether.

V. WHAT COURTS SHOULD DO

This Comment has demonstrated that courts, commentators, and legislators treat customer lists differently for online and offline companies. The Comment has also argued that this separate treatment is both unwarranted and harmful.[140] This Part argues that courts confronted with cases involving customer lists should recognize the substantial existing case law and focus on contract, rather than privacy, law. Future legislation, moreover, should concentrate on *how* cus-

---

did not demonstrate adequate respect for privacy. . . . The FTC, then, is able to indirectly promote its goal of data privacy by getting large websites to do its bidding.

137 See Parts III.A and III.D.

138 See Part II.

139 One way that online companies have attempted to respond to the uncertainty is by rewording and removing their disclosure policies to permit the sale of information in the event of a sale or liquidation of the company. Tamara Loomis, *Amazon Revamps Its Policy on Sharing Data*, NY L J 5 (Sept 21, 2000) (noting that Amazon.com rewrote its privacy policy after learning of Toysmart.com's inability to sell its list).

140 See Part IV.

tomer information is used, instead of the medium through which it is collected.

A. Recognize the Substantial Body of Case Law That Exists

Before getting caught up in the public's increasing concern over customer privacy, courts should recognize that there is a substantial body of case law that protects a company's right to its customer list.[141] For over fifty years, the law has protected a company's right to create customer lists[142] and has allowed those lists to be freely alienable.[143] By indicating that courts will not interfere, these judicial decisions provided an important incentive for companies to gather information about customer preferences. Consequently, companies have been able to provide customers with more focused marketing and better service.[144]

There will likely be changes in privacy laws in the future. In fact, many of the current legislative proposals treat data gathered online differently from data gathered from other sources.[145] However, the decision to distinguish between online and offline companies, if made at all, should be confined to the legislature. By ignoring precedent and distinguishing between online and offline customer lists, courts will only create distortions in the market, produce complex and expensive litigation, and cause conflicting judicial decisions.

B. Contracts, Not Privacy

Once the rhetoric dies away, most of the cases involving online customer lists will likely turn on the interpretation of the companies' privacy policies. As the *Toysmart.com* litigation illustrated, a privacy policy that promises not to "share information with third parties" leaves a lot open for interpretation. The central issue in customer list cases should be whether the company breached a contract with customers,"not whether the customer has a privacy or property right to the information."[146]

Returning the focus of the debate to contract law will also permit the market to have a greater impact on privacy issues. If customers

---

141 See Part II.

142 See id.

143 See id.

144 See Part III.C.

145 See Part I.D.

146 For commentary on the treatment of customer lists in bankruptcy and in contract law, see generally Andrew B. Buxbaum and Louis A. Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (But Not under the Bankruptcy Code)*, 8 Am Bankr Inst L Rev 395 (2000). See also Miller and O'Rourke, 38 Houston L Rev at 795–807 (cited in note 61) (discussing the contractual aspects of customer lists).

demand privacy policies, they can patronize those companies that post the policies and boycott those that do not. The market has already had tremendous success in encouraging companies to post privacy policies in the first place.[147] Now customer groups can refocus their attention by ensuring that the policies are appropriately worded and that they are adopted by both large and small companies. While the policies can be adopted online and offline, courts will not have to differentiate among technologies. Instead, they can simply enforce contracts. Courts have already applied this reasoning successfully to offline companies.[148] If the sale of customer lists were analyzed through contract principles, the results of high-profile bankruptcies like that of Toysmart.com and Living.com might have been very different. Instead, discussion focused on property rights in private information,[149] thereby creating a counterproductive result that favors large companies over small.

C. Guidelines for Future Legislation

Customers have legitimate reasons for wanting to prohibit the collection and use of certain types of customer information. Protecting child privacy and limiting the distribution of health records, for instance, might be extremely important goals regardless of whether the information is distributed online or offline. These policies, however, should not depend on where the information was gathered. While customer advocates may argue that technology makes abuse more likely online, companies do not cause harm merely by gathering or transmitting information.

Customer privacy can only be violated through the *use* of that information. Although privacy advocates have focused on the collection of information with the understandable belief that the information is being gathered so that it can be used, punishing the collection of information is the wrong approach. Regulators can avoid the technology split and also provide the appropriate level of protection simply by requiring customers to demonstrate a way in which their information was used that materially harmed them or violated a current law.

Consumers have a variety of causes of action depending on what kind of information was used, as well as how it was used. For instance, the Health Insurance Portability and Accountability Act protects against the distribution of certain health information.[150] The Children's

---

147 For a general discussion, see Hetcher, 7 Mich Telecomm & Tech L Rev 97 (cited in note 4) (developing a case study of website privacy norms and examining how market forces have shaped and enforced these norms).

148 See Part II.

149 See text accompanying notes 38–46.

150 See the Health Insurance Portability and Accountability Act ("HIPAA"), Pub L No 104-191, 110 Stat 1939 (1996), codified at 29 USC § 1181 et seq (1994 & Supp 1999) (protecting the

Online Privacy Protection Act[151] limits the companies' ability to use information about children.[152] Content-based laws such as these will be more effective than those based purely on whether the information was gathered online or offline.

CONCLUSION

It is tempting to believe that the technological revolution has dramatically changed the world over the last several decades, and in many ways, the world is dramatically different. However, the law of customer lists is at least one subject where courts can benefit by studying previous case law and applying existing legal structures to help them answer today's issues. Perpetuating a technology split is counterproductive. Instead, lawyers, judges, regulators, and customer advocates who are concerned about privacy should recognize that a substantial body of case law on customer lists exists, and they should focus on policing contracts rather than on advocating new privacy rights. Finally, whether information is sensitive does not depend on how it was transmitted, but on the nature of the information. This Comment has advocated that courts and legislators should focus, not on the method by which customer information is gathered, but on how that information will be used.

---

privacy of certain health information); Letter by Direction of Commission to the U.S. Department of Health and Human Services Assistant Secretary for Planning and Evaluation (Feb 17, 2000), available online at <http://www.ftc.gov/be/v000001.htm> (visited June 12, 2002) (describing proposed privacy standards under HIPAA).

151 Children's Online Privacy Protection Act, Pub L No 105-277, 112 Stat 2681–728 (1998), codified at 15 USC § 6501 et seq (2000) (establishing rules for the regulation of practices in connection with the collection and use of information from and about children on the Internet). See also *Ashcroft v ACLU*, 122 S Ct 1700 (2002) (upholding a portion of COPA but remanding for further consideration); Title V of the Disclosure of Nonpublic Personal Information, Pub L No 106-102, 113 Stat 1436 (1999), codified at 15 USC §§ 6801–10 (2000) (promulgating standards for the use of private information in the financial industry).

152 Although the Act applies to online companies, the focus is on a type of information, not a transportation medium.